UNITED STATES DISTRICT COURT

for the
Eastern District of Wisconsin

In the Matter of the Search of:

information associated with Apple ID rock2don@yahoo.com that is stored at premises controlled by Apple.

Case No. 19-MJ-1215

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property:

See Attachment A.

located in the Eastern District of Wisconsin, there is now concealed:

See Attachment B.

The basis for the search under Fed. R. Crim P. 41(c) is:

- ■ evidence of a crime;
- ☐ contraband, fruits of crime, or other items illegally possessed;
- ☐ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to violations of: Title 18, United States Code, Section 844(i); Title 18, United States Code, Section 844(m); Title 18, United States Code, Section 1519

The application is based on these facts: See attached affidavit.

☐ Delayed notice of _____ days (give exact ending date if more than 30 days:_____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

Special Agent Rick Hankins of the ATF
Printed Name and Title

Sworn to before me and signed in my presence:

Date: 3/5/19

Judge's signature

City and State: Milwaukee, Wisconsin

Honorable William E. Duffin, U.S. Magistrate Judge
Printed Name and Title

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT

I, Rick Hankins, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Apple Inc. (hereafter "Apple") to disclose to the government records and other information, including the contents of communications, associated with the above-listed Apple ID that is stored at premises owned, maintained, controlled, or operated by Apple, a company headquartered at 1 Infinite Loop, Cupertino, California. The information to be disclosed by Apple and searched by the government is described in the following paragraphs and in Attachments A and B.

2. I am a Special Agent of the U.S. Department of Justice's Bureau of Alcohol, Tobacco, Firearms, and Explosives (ATF), currently assigned to the Milwaukee Field Office. I have been so employed since April 2003. My duties as a Special Agent with the ATF include investigating alleged violations of the federal firearms, explosives, and arson statutes.

3. I have completed approximately 26 weeks of training at the Federal Law Enforcement Training Center in Glynco, Georgia, as well as the ATF National Academy. That training included various legal courses related to constitutional law as well as search and seizure authority. Additionally, I have received training on how to conduct various tasks associated with criminal investigations, such as interviewing, surveillance, and evidence collection.

4. In addition to my duties as a criminal investigator, I am also an ATF Certified Fire Investigator (CFI). As an ATF CFI, I am tasked with providing expert opinions as to the origin and cause of fires. I obtained the ATF CFI certification in 2009 following a two-year training

program that centered on various fire science topics including, but not limited to: chemistry, fire dynamics, and building construction. The two-year ATF CFI certification program consisted of college courses, written exams, research papers, reading assignments, practical training exercises, and test burns of various materials. I am re-certified annually as an ATF CFI. To date, I have participated in over 255 fire scene examinations and have testified as an expert. Additionally, I have been certified as a fire investigator by the International Association of Arson Investigators since June 2011. I have received over 1,200 class hours of fire-related training. Furthermore, I have been an instructor regarding fire-related topics on multiple occasions for the following agencies and institutions: The National Fire Academy (FEMA), International Association of Arson Investigators Chapter 25, Waukesha County Technical College, Milwaukee Area Technical College, and Blackhawk Technical College. I have also participated in over 185 live fire training exercises, where I started training fires and observed fire growth and development. Finally, I was a full-time instructor at the ATF National Academy from approximately August 2015 to August 2016, where I taught several topics during Special Agent Basic Training for new ATF recruits. Specifically, I was a primary instructor for the arson block of training at the ATF Academy.

5. I am an investigative or law enforcement officer of the United States within the meaning of Section 2510(7) of Title 18, United States Code, in that I am empowered by law to conduct investigations of and to make arrests for federal offenses. As a part of my duties with the ATF, I investigate criminal violations relating to arson and arson-related offenses, including violations of Title 18, United States Code, Section 844. During the course of my investigations, I have regularly used electronic evidence relating to the commission of criminal offenses, including intent, motive, manner, means, and the identity of co-conspirators.

6. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses. This affidavit is also based upon information gathered from interviews of citizen witnesses, reports, official records, law enforcement reports, and information provided to me by other federal, state, and local law enforcement officers. This affidavit is intended to show simply that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

7. Based on the facts as set forth in this affidavit, there is probable cause to believe that the information described in Attachment A contains evidence of violations of arson of commercial property, in violation of Title 18, United States Code, Section 844(i), conspiracy to commit arson, in violation of Title 18, United States Code, Section 844(m), and destruction, alteration, or falsification of records in federal investigations, in violation of Title 18, United States Code, Section 1519, as described in Attachment B.

JURISDICTION

8. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A), & (c)(1)(A). Specifically, the Court is "a district court of the United States . . . that has jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3)(A)(i).

PROBABLE CAUSE

9. In conjunction with other federal, state, and local law enforcement officers, I am conducting an investigation into an arson affecting interstate commerce and a conspiracy to commit arson that occurred on January 2, 2019 in the vicinity 716 West Rogers Street in Milwaukee, Wisconsin, in violation of Title 18, United States Code, Sections 844(i) and 844(m).

10. On January 2, 2019 at approximately 9:55 p.m., the Milwaukee Fire Department and the Milwaukee Police Department responded to a vehicle fire in the vicinity of 716 West Rogers Street in Milwaukee, Wisconsin. The vehicle was identified as a 2001 Ford F-250 pickup truck bearing Wisconsin license plate MA-9985 and Vehicle Identification Number 1FTNW21L21EC43063. Police officers were informed that the fire was suspicious.

11. A registration check with the Wisconsin Department of Motor Vehicles revealed that the Ford F-250 pickup truck bearing Wisconsin license plate MA-9985 is registered to Matthew Neumann (DOB: XX/XX/1975), who lives at 9426 South 29th Street in Franklin, Wisconsin.

12. At about 11:00 p.m. on January 2, 2019, police officers of the Franklin Police Department contacted Matthew Neumann at his residence. One officer noticed a strong odor of a chemical accelerant, once let inside by Matthew Neumann, and observed clothing lying nearby. Matthew Neumann told the police officers that he owns eight trucks, because he owns a plowing business and that he lets one of his employees drive the Ford F-250 home.

13. Police officers later interviewed Matthew Neumann's family. Tammy Neumann, Matthew Neumann's wife, stated that at approximately 5:00 a.m. on January 2, 2019 she was awoken by Matthew Neumann at their residence at 9426 South 29th Street in Franklin, Wisconsin. She observed that Matthew Neumann was intoxicated and began undressing, and she also noticed that Matthew Neumann had a black handgun and heard him rack the slide.

14. When she left the house later that morning, Tammy Neumann observed Matthew Neumann's 2001 Ford F-250 pickup truck bearing Wisconsin license plate MA-9985 parked on the driveway and observed a white male, approximately 35 to 40 years old, slumped down in the passenger seat. Tammy Neumann looked through the window and observed no signs of life. She

thought that the male had blood around his nose and mouth and that the passenger window may have been spidered, as if struck by a human head.

15. According to Tammy Neumann, Matthew Neumann did not return to the residence until about 10:00 p.m. that night. When he did, Tammy Neumann smelled a strong odor of diesel fuel on Matthew Neumann's clothes, such that she told Matthew Neumann to put the clothes outside.

16. Matthew Neumann's daughter overheard a conversation between Tammy Neumann and Matthew Neumann, where Matthew Neumann said that he shot "Rich" or "Dick" "over a pack of squares." Tammy Neumann and her daughter left the residence and later returned. At that point, the truck was gone along with Matthew Neumann.

17. On January 8 and 11, 2019, I conducted a fire scene examination of the Ford F-250 along with the Milwaukee Police Department and Wisconsin Department of Justice's Division of Criminal Investigation pursuant to a state search warrant. One officer discovered a bullet hole and strike on the B-pillar of the passenger side of the pickup truck, a lead bullet fragment at the base of the B-pillar in the midst of fire debris, and other lead bullet fragments on the B-pillar. Using a trajectory rod, another officer determined that the bullet traveled from the driver seat area to the B-pillar of the passenger seat. Officers also located a bullet and casings inside of a black melted mass on the driver's side floorboard. I located blood along the weather stripping on the passenger floorboard, removed the passenger seat, and observed additional blood on the flooring and carpeting. I also recovered fire debris from the backseat area that emitted an odor consistent with that of a petroleum distillate.

18. The ATF Forensic Laboratory later analyzed fire debris samples recovered from the truck bed and the backseat area of the Ford F-250. The laboratory results showed the presence of gasoline in the truck bed and back seat area of the Ford F-250.

19. I also obtained surveillance video that captured Matthew Neumann drive the Ford F-250 into the Citgo gas station located at 610 West Becher Street at 9:44 p.m. on January 2, 2019, followed by an early 2000s maroon Chevrolet Impala. Matthew Neumann purchased cigarettes and a lighter at the Citgo gas station. The Ford F-250 and Chevrolet Impala subsequently disappeared east out of the video frame.

20. At approximately 9:47 p.m., a second surveillance video captured the Ford F-250 turn westbound on Rogers Street from South 6th Street, followed by the Chevrolet Impala. The Ford F-250 parked westbound on Rogers Street immediately east of 1978 South 8th Street. The driver's door of the Ford F-250 subsequently opened, Matthew Neumann exited, and a clear illumination appears inside of the Ford F-250 at 9:48 p.m. as the Chevrolet Impala passed. The Chevrolet Impala traveled westbound on Rogers Street and turned southbound on 8th Street, stopping south of the intersection. There was a sudden and intense sustained flash of light inside the Ford F-250 as Matthew Neumann walked and then ran to the parked Chevrolet Impala and entered the passenger side of the Impala. The Impala then drove away. The Impala was captured on surveillance video traveling south on 8th Street away from the burning truck and then west on Becher Street.

21. After examining the Ford F-250, reviewing the surveillance videos, and obtaining laboratory results, I determined that the fire was the result of the human introduction of a heat source to available combustible material inside the passenger compartment of the Ford F-250,

including the presence of an ignitable liquid. Based on my knowledge, training, and experience, I conclude this fire was incendiary.

22. Officers also recovered the clothing that Matthew Neumann had been wearing when he returned home on January 2, 2019. That clothing contained the odor of diesel fuel, blood in several areas, and a burn area. That clothing also matched the clothing Matthew Neumann was seen wearing on the Citgo gas station surveillance video minutes prior to the Ford F-250 fire.

23. During an interview with officers on January 10, 2019, Matthew Neumann admitted to starting the fire of the Ford F-250, claiming that he did so accidentally. He claimed that, after the vehicle fire, another vehicle in the area picked him up and that he paid the driver $30 to $40 to take him to a tavern close to his home. Matthew Neumann claimed that the driver of the vehicle was a white male and that the vehicle was burgundy or maroon in color and from the late 1990s or early 2000s—this description is consistent with that of Donald Neumann and Donald Neumann's 2003 Chevrolet Impala.

24. Officers later executed a search warrant on hunting land leased by Matthew Neumann in the Mukwonago area and located a black-and-white Spot Free Cleaning trailer. Next to the trailer was a burn pit containing the heavily charred remains of two individuals, along with other items such as charcoal and charcoal bags.

25. Officers of the Franklin Police Department recovered surveillance video from the Home Depot in Mukwonago, approximately five miles from Matthew Neumann's hunting property, which depicts Matthew Neumann alone on January 3, 2019 at 10:58 a.m. purchasing four bags of charcoal, lighter fluid, and eight pieces of lumber.

26. According to publicly available court records, the State of Wisconsin charged Matthew Neumann with First-Degree Reckless Homicide, in violation of Wisconsin Statute

940.02, and Mutilating or Hiding a Corpse, in violation of Wisconsin Statute 940.11(2), in Milwaukee County Case No. 2019CF000204.

27. Based on subscriber information, telephone toll records, and historical cell site information obtained pursuant to state search warrants, I know that Matthew Neumann's primary phone is an Apple iPhone assigned call number 414-350-7417 with service provided by Sprint. When Matthew Neumann was arrested, however, he was in possession of an Alcatel 5041C cell phone with an assigned call number 414-687-5095 with service provided by AT&T. This appears to have been what is commonly referred to as a "burner phone," in that this is a prepaid cellphone with service starting on or about January 4, 2019.

28. A CLEAR search indicates that Donald Neumann is associated with the call number 414-899-6082. Detective Jason Ireland of the Franklin Police Department also identified 414-899-6082, as the contact number used to communicate with Donald Neumann. Detective Ireland has communicated with Donald Neumann multiple times during this investigation on that call number, and I have too. This is corroborated by the subscriber information, telephone toll records, and historical cell site information provided by Sprint for Donald Neumann's phone number.

29. The cell site and telephone toll records show that Matthew Neumann and Donald Neumann exchanged approximately 17 phone communications between 8:02 p.m. and 9:38 p.m. on January 2, 2019. Notably, Matthew Neumann had no other contact with any other number during that time period.

30. An Intelligence Analyst from the Milwaukee County District Attorney's Office reviewed cell site and telephone toll records for Donald Neumann's phone number 414-899-6082. Cell site maps prepared by the Milwaukee County District Attorney's Office indicate that Donald Neumann's cellphone was in the vicinity of 716 West Rogers Street at about the time of the arson

on January 2, 2019, because his cellphone used multiple cell towers and sectors in and around that location. These pings on the cell site maps are also consistent with Matthew Neumann's cell site and telephone toll records, which indicate multiple calls on or about those times.

31. I know that Donald Neumann has a registered address in the Eastern District of Wisconsin. I have reviewed records from the Wisconsin Department of Transportation, which show that he registered a red 2003 Chevrolet Impala on November 30, 2018 and listed a mailing address of W141N513 Ridgeway Lane in Menomonee Falls, Wisconsin 53051. A CLEAR search also indicates that Donald Neumann registered a red 2003 Chevrolet Impala bearing Wisconsin license plate AEE-6205 on or about November 30, 2018 with a registered mailing address of W141N513 Ridgeway Lane, Menomonee Falls, Wisconsin 53051.

32. On or about January 21, 2019, the Milwaukee Police Department executed a search warrant on Donald Neumann's maroon 2003 Chevrolet Impala. The officers found that the interior of the vehicle had recently been deep cleaned. I compared the photos of Donald Neumann's seized Chevrolet Impala to the surveillance video on the night of the truck fire. There were no dissimilarities in the appearances of the two vehicles. In fact, the color, wheel rims, and trunk spoiler appeared consistent with one another.

33. On February 1, 2019, this Court issued a search warrant authorizing the search of Donald Neumann's person for the seizure of the cellular device assigned phone number 414-899-6082. On February 4, 2019, I observed Donald Neumann using the cellular device assigned phone number 414-899-6082 in front of his residence, located at W141N513 Ridgeway Lane in Menomonee Falls, Wisconsin 53051. I seized his cellphone—an Apple iPhone.

34. On February 11, 2019, this Court issued a warrant authorizing the forensic examination of Donald Neumann's Apple iPhone. Pursuant to that search warrant, Special Agent Undre Ludington of the ATF extracted information from the cellphone.

35. The forensic extraction report indicates that the Apple ID associated with that phone is rock2don@yahoo.com, that an iCloud account is present, and that the MSISDN associated with that phone is 4148996082. The report also indicates that the cellular device was used to send a text message on February 1, 2019 referring to Donald Neumann's 2003 Chevrolet Impala, stating in substance: "You know my brother has not sat in that car for 10 days Since I picked him up our car has been anywhere and everywhere. Sent this to lawyer too." Officers of the Milwaukee Police Department and Franklin Police Department seized Donald Neumann's 2003 Chevrolet Impala on January 13, 2019—approximately 10 days after the arson on January 2, 2019.

36. A comparison of the forensic extraction report for Donald Neumann's Apple iPhone and the cell site and toll records for Donald Neumann's call number 414-899-6082, the call number assigned to that same cellphone, indicates that relevant electronic evidence immediately prior to the arson was deleted from the cellphone.

37. The forensic extraction report indicates that 76 locations, 24 notes, 87 searched items, and 121 web history items were deleted. The phone's log entries indicate data usage on December 29, 2019, January 2, 2019, January 4, 2019, January 5, 2019, January 7, 2019, January 8, 2019, and January 10, 2019. However, the Chrome search history only dates back to January 3, 2019, the day after the arson. No Chrome search history prior to that date is contained in the forensic extraction report, even though the report indicates numerous Chrome searches after that date until the seizure of the cell phone. Donald Neumann's cell phone also contains records of

Safari searches, but only prior to November 19, 2017. There is no search history from November 19, 2017 to January 3, 2019—more than a one-year gap. This suggests that the Chrome search history prior to the arson was deleted.

38. The same is true of call and text message history. The call history contains records of incoming and outgoing phone calls after January 29, 2019. In fact, the forensic extraction report indicates that Donald Neumann made or received 189 calls between January 29, 2019 and February 4, 2019—the date I seized the phone. There are no records of phone calls made using the call number 414-899-6082 prior to January 29, 2019 contained in the forensic extraction report. There are, however, sporadic calls made or received using Facebook Messenger prior to that date.

39. Likewise, the MMS message history only includes messages from January 15, 2019 to January 30, 2019; there are no MMS messages prior to this date. The SMS message history includes messages from January 15, 2019 to February 4, 2019; there are no SMS messages prior to this date.

40. The username rock2don@yahoo.com was first used as a User Account on the cellphone on November 28, 2014, according to the forensic extraction report. The forensic extraction report also indicates that a contact numbers for a "Spoty," a "Tammy Cell", a "Spot," a "Saukville Sue," a "Sherwin Brookfield," a "Sherwin 124th St.," a "Sherwin West Alis," a "Sherwin Grafton," a "Sherwin Pewaukee," and a "Matt & Tammy" contain a timestamp of April 11, 2013. I know that Donald Neumann is a painter by profession. The contact photo for "Matt & Tammy" contains a photograph of Matthew Neumann, and that contact was created on April 11, 2013.

41. As a result of witness interviews, business records, and search warrant executions, I also know that Matthew Neumann's Ford F-250 was a business vehicle in the name of Spot Free Cleaning and that the Ford F-250 was regularly used in or affecting interstate commerce.

42. Matthew Neumann's address—9426 South 29th Street in Franklin, Wisconsin—and cell phone number 414-350-7417 are also the listed contact information for Spot Free Cleaning Solutions on the publicly available listing on Angie's List (https://www.angieslist.com/companylist/us/wi/franklin/spot-free-cleaning-solutions-reviews-6459566.htm) (last viewed on January 31, 2019). The description of Spot Free Cleaning on Angie's List is as follows:

> Commercial Cleaning Every masterpiece begins with a crystal clear canvas and the same goes for your business. Whatever your trade, the appearance and cleanliness of your facility are of the utmost importance to customers, employees and the general public. Get your competitive edge at an affordable price with Spot Free Cleaning! When it comes to professionalism and success, it's all about first impressions. With state-of-the-art equipment and over 17 years of commercial cleaning experience, Spot Free guarantees that a first impression will be the last thing on your mind. Sign up for our daily, weekly or monthly cleaning programs to keep your cleaning woes out of sight-out of mind. We offer 24 hour service, 365 days a year! We offer a full range of services including floor care, carpet cleaning, window cleaning, pressure washing and snow plowing. The Spot Free Cleaning difference is simple-we go the extra mile. From the shine of your showroom to a pristine parking lot, you can count on us to get the job done.

43. Matthew Neumann's cell phone number 414-350-7417 is also the listed contact information for Spot Free Cleaning on the publicly available listing on Yelp (https://www.yelp.com/biz/spot-free-cleaning-franklin-2) (last viewed on January 31, 2019).

44. During my fire scene examination, I observed a plow mount on the front end of the Ford F-250, along with a power and control tether for a plow that ran into the passenger compartment of the truck.

45. On January 8, 2019, the Franklin Police Department executed a search warrant at the business address for Spot Free Cleaning. The officers found two work trucks, both with plows attached to their front ends. The photos from that search warrant also show a third plow unattached to a vehicle on the ground. There were no other vehicles at the business location equipped with a plow mount. I believe that the unattached plow found during this search warrant execution had likely been used with the Ford F-250 pickup truck bearing Wisconsin license plate MA-9985.

46. During that search, police officers also recovered business records from Spot Free Cleaning. Those records indicate that Spot Free Cleaning had performed salting and plowing services from at least November 15, 2018 through January 2, 2019. Those records also include contract(s) and addenda between Spot Free Cleaning and Reliable Property Services for a winter snow removal service for the 2018-2019 season. Those documents appear to be signed by Matthew Neumann.

47. On January 29, 2019, police officers from the Franklin Police Department spoke with Tammy Neumann and Matthew Neumann, Jr., who indicated that the Ford F-250 pickup truck was used for business purposes by Spot Free Cleaning, that all employees were allowed to drive and use the Ford F-250 pickup truck for business purposes, and that the Ford F-250 pickup truck was used for snow plowing. Matthew Neumann, Jr. indicated that the Ford F-250 had been used during the winter of 2017-2018, but had not been used during the winter of 2018-2019 because there had not been enough snow.

48. A transaction record from Summit Credit Union shows a business loan in the name of Spot Free Cleaning was issued for a 2001 Ford on or about December 31, 2016, that regular payments have been made since, and that, as of July 20, 2018, a nearly $4,000 balance remained.

49. Insurance documents provided by 1st Auto & Casualty Insurance Company indicates that Matthew Neumann's 2001 Ford F-250 bearing the same Vehicle Identification Number was insured as a business vehicle for Spot Free Cleaning with a policy period of February 18, 2018 to February 18, 2019.

INFORMATION REGARDING APPLE ID AND iCLOUD[1]

50. Apple is a United States company that produces the iPhone, iPad, and iPod Touch, all of which use the iOS operating system, and desktop and laptop computers based on the Mac OS operating system.

51. Apple provides a variety of services that can be accessed from Apple devices or, in some cases, other devices via web browsers or mobile and desktop applications ("apps"). As described in further detail below, the services include email, instant messaging, and file storage:

a. Apple provides email service to its users through email addresses at the domain names mac.com, me.com, and icloud.com.

b. iMessage and FaceTime allow users of Apple devices to communicate in real-time. iMessage enables users of Apple devices to exchange instant messages ("iMessages")

[1] The information in this section is based on information published by Apple on its website, including, but not limited to, the following document and webpages: "U.S. Law Enforcement Legal Process Guidelines," available at http://images.apple.com/privacy/docs/legal-process-guidelines-us.pdf; "Create and start using an Apple ID," available at https://support.apple.com/en-us/HT203993; "iCloud," available at http://www.apple.com/icloud/; "What does iCloud back up?," available at https://support.apple.com/kb/PH12519; "iOS Security," available at https://www.apple.com/business/docs/iOS_Security_Guide.pdf, and "iCloud: How Can I Use iCloud?," available at https://support.apple.com/kb/PH26502.

containing text, photos, videos, locations, and contacts, while FaceTime enables those users to conduct video calls.

c. iCloud is a file hosting, storage, and sharing service provided by Apple. iCloud can be utilized through numerous iCloud-connected services, and can also be used to store iOS device backups and data associated with third-party apps.

d. iCloud-connected services allow users to create, store, access, share, and synchronize data on Apple devices or via icloud.com on any Internet-connected device. For example, iCloud Mail enables a user to access Apple-provided email accounts on multiple Apple devices and on icloud.com. iCloud Photo Library and My Photo Stream can be used to store and manage images and videos taken from Apple devices, and iCloud Photo Sharing allows the user to share those images and videos with other Apple subscribers. iCloud Drive can be used to store presentations, spreadsheets, and other documents. iCloud Tabs and bookmarks enable iCloud to be used to synchronize bookmarks and webpages opened in the Safari web browsers on all of the user's Apple devices. iWork Apps, a suite of productivity apps (Pages, Numbers, Keynote, and Notes), enables iCloud to be used to create, store, and share documents, spreadsheets, and presentations. iCloud Keychain enables a user to keep website username and passwords, credit card information, and Wi-Fi network information synchronized across multiple Apple devices.

e. Game Center, Apple's social gaming network, allows users of Apple devices to play and share games with each other.

f. Find My iPhone allows owners of Apple devices to remotely identify and track the location of, display a message on, and wipe the contents of those devices. Find My Friends allows owners of Apple devices to share locations.

g. Location Services allows apps and websites to use information from cellular, Wi-Fi, Global Positioning System ("GPS") networks, and Bluetooth, to determine a user's approximate location.

h. App Store and iTunes Store are used to purchase and download digital content. iOS apps can be purchased and downloaded through App Store on iOS devices, or through iTunes Store on desktop and laptop computers running either Microsoft Windows or Mac OS. Additional digital content, including music, movies, and television shows, can be purchased through iTunes Store on iOS devices and on desktop and laptop computers running either Microsoft Windows or Mac OS.

52. Apple services are accessed through the use of an "Apple ID," an account created during the setup of an Apple device or through the iTunes or iCloud services. A single Apple ID can be linked to multiple Apple services and devices, serving as a central authentication and syncing mechanism.

53. An Apple ID takes the form of the full email address submitted by the user to create the account; it can later be changed. Users can submit an Apple-provided email address (often ending in @icloud.com, @me.com, or @mac.com) or an email address associated with a third-party email provider (such as Gmail, Yahoo, or Hotmail). The Apple ID can be used to access most Apple services (including iCloud, iMessage, and FaceTime) only after the user accesses and responds to a "verification email" sent by Apple to that "primary" email address. Additional email addresses ("alternate," "rescue," and "notification" email addresses) can also be associated with an Apple ID by the user.

54. Apple captures information associated with the creation and use of an Apple ID. During the creation of an Apple ID, the user must provide basic personal information including the user's full name, physical address, and telephone numbers. The user may also provide means of payment for products offered by Apple. The subscriber information and password associated with an Apple ID can be changed by the user through the "My Apple ID" and "iForgot" pages on Apple's website. In addition, Apple captures the date on which the account was created, the length of service, records of log-in times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to and utilize the account, the Internet Protocol address ("IP address") used to register and access the account, and other log files that reflect usage of the account.

55. Additional information is captured by Apple in connection with the use of an Apple ID to access certain services. For example, Apple maintains connection logs with IP addresses that reflect a user's sign-on activity for Apple services such as iTunes Store and App Store, iCloud, Game Center, and the My Apple ID and iForgot pages on Apple's website. Apple also maintains records reflecting a user's app purchases from App Store and iTunes Store, "call invitation logs" for FaceTime calls, "query logs" for iMessage, and "mail logs" for activity over an Apple-provided email account. Records relating to the use of the Find My iPhone service, including connection logs and requests to remotely lock or erase a device, are also maintained by Apple.

56. Apple also maintains information about the devices associated with an Apple ID. When a user activates or upgrades an iOS device, Apple captures and retains the user's IP address and identifiers such as the Integrated Circuit Card ID number ("ICCID"), which is the

serial number of the device's SIM card. Similarly, the telephone number of a user's iPhone is linked to an Apple ID when the user signs in to FaceTime or iMessage. Apple also may maintain records of other device identifiers, including the Media Access Control address ("MAC address"), the unique device identifier ("UDID"), and the serial number. In addition, information about a user's computer is captured when iTunes is used on that computer to play content associated with an Apple ID, and information about a user's web browser may be captured when used to access services through icloud.com and apple.com. Apple also retains records related to communications between users and Apple customer service, including communications regarding a particular Apple device or service, and the repair history for a device.

57. Apple provides users with five gigabytes of free electronic space on iCloud, and users can purchase additional storage space. That storage space, located on servers controlled by Apple, may contain data associated with the use of iCloud-connected services, including: email (iCloud Mail); images and videos (iCloud Photo Library, My Photo Stream, and iCloud Photo Sharing); documents, spreadsheets, presentations, and other files (iWork and iCloud Drive); and web browser settings and Wi-Fi network information (iCloud Tabs and iCloud Keychain). iCloud can also be used to store iOS device backups, which can contain a user's photos and videos, iMessages, Short Message Service ("SMS") and Multimedia Messaging Service ("MMS") messages, voicemail messages, call history, contacts, calendar events, reminders, notes, app data and settings, Apple Watch backups, and other data. Records and data associated with third-party apps may also be stored on iCloud; for example, the iOS app for WhatsApp, an instant messaging service, can be configured to regularly back up a user's instant messages on

iCloud Drive. Some of this data is stored on Apple's servers in an encrypted form but can nonetheless be decrypted by Apple.

a. In my training and experience, evidence of who was using an Apple ID and from where, and evidence related to criminal activity of the kind described above, may be found in the files and records described above. This evidence may establish the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or, alternatively, to exclude the innocent from further suspicion. As described above, the toll records and cell site data for Donald Neumann's call number and Matthew Neumann's call number indicate that they exchanged multiple communications around the time of the arson on January 2, 2019 and that some of those communications were routed through cell towers and sectors in the vicinity of the arson. This information, however, is not reflected in the forensic extraction report for Donald Neumann's cell phone, including the call history, MMS history, SMS history, location information, and GPS history. As described above, the forensic extraction report indicates that multiple items have been deleted from Donald Neumann's Apple iPhone, which is material to Donald Neumann's intent, knowledge, and state of mind.

b. However, the communications contained in Donald Neumann's Apple iCloud account (including iMessage and Facetime), along with the approximate location of Donald Neumann's Apple iPhone (as determined from Find My iPhone, Find My Friends, cellular, Wi-Fi, and Global Positioning System (GPS) networks, and Bluetooth), on the date of the arson compared to the weeks before and after the arson, between Donald Neumann and Matthew Neumann are material to determining Donald Neumann's involvement in the arson on

January 2, 2019. That information is material to establish whether Donald Neumann and Matthew Neumann acted-in-concert, by establishing the nature and extent of their relationship, the scope of the conspiracy, the pattern of their communications, their patterns of travel, and any deviations from those patterns.

58. For example, the stored communications and files connected to an Apple ID may provide direct evidence of the offenses under investigation. Based on my training and experience, instant messages, emails, voicemails, photos, videos, and documents are often created and used in furtherance of criminal activity, including to communicate and facilitate the offenses under investigation. The instant messages, emails, voicemails, photos, videos, and documents contained on Donald Neumann's Apple iCloud account are likely to provide evidence of these crimes. By comparing the information from the Apple iCloud account linked to Donald Neumann's cellphone and the information contained on the device, this information will also provide material evidence about means, manner, and intent of any alteration or destruction of records, documents, or tangible objects.

59. In addition, the user's account activity, logs, stored electronic communications, and other data retained by Apple can indicate who has used or controlled the account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. "User attribution" evidence is material to determining the custody, possession, and control of Donald Neumann's Apple iPhone around the date of the arson. Evidence of who has used or controlled the account is relevant to determining the location of the cellular device associated with Donald Neumann's Apple ID. For example, subscriber information, email and messaging logs, documents, and photos and videos (and the data

associated with the foregoing, such as geo-location, date and time) may be evidence of who used or controlled the account at a relevant time. As an example, because every device has unique hardware and software identifiers, and because every device that connects to the Internet must use an IP address, IP address and device identifier information can help to identify which computers or other devices were used to access the account. Such information also allows investigators to understand the geographic and chronological context of access, use, and events relating to the crime under investigation.

60. Account activity may also provide relevant insight into the account owner's state of mind as it relates to the offenses under investigation. For example, information on the account may indicate the owner's motive and intent to commit a crime (e.g., information indicating a plan to commit a crime), or consciousness of guilt (e.g., deleting account information in an effort to conceal evidence from law enforcement).

61. Other information connected to an Apple ID may lead to the discovery of additional evidence. For example, the identification of apps downloaded from App Store and iTunes Store may reveal services used in furtherance of the crimes under investigation or services used to communicate with co-conspirators. In addition, emails, instant messages, Internet activity, documents, and contact and calendar information can lead to the identification of co-conspirators and instrumentalities of the crimes under investigation.

62. I know that Assistant United States Attorney Philip T. Kovoor served Apple, Inc. with a preservation letter on March 1, 2019 for the information sought in this warrant.

63. Therefore, Apple's servers are likely to contain stored electronic communications and information concerning subscribers and their use of Apple's services. In my training and experience, such information may constitute evidence of the crimes under investigation including information that can be used to identify the account's user or users.

INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED

64. I anticipate executing this warrant under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), by using the warrant to require Apple to disclose to the government copies of the records and other information (including the content of communications and stored data) particularly described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

CONCLUSION

65. Based on the forgoing, I request that the Court issue the proposed search warrant.

66. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant.

REQUEST FOR SEALING

67. I further request that the Court order that all papers in support of this application, including the affidavit and search warrant, be sealed until further order of the Court. These documents discuss an ongoing criminal investigation that is neither public nor known to all of

the targets of the investigation. Accordingly, there is good cause to seal these documents because their premature disclosure may seriously jeopardize that investigation.

ATTACHMENT A

Property to Be Searched

This warrant applies to information associated with Apple ID rock2don@yahoo.com (the "account") that is stored at premises owned, maintained, controlled, or operated by Apple Inc., a company headquartered at Apple Inc., 1 Infinite Loop, Cupertino, CA 95014.

ATTACHMENT B

Particular Things to be Seized

I. Information to be disclosed by Apple

To the extent that the information described in Attachment A is within the possession, custody, or control of Apple, regardless of whether such information is located within or outside of the United States, including any messages, records, files, logs, or information that have been deleted but are still available to Apple, or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Apple is required to disclose the following information to the government, in unencrypted form whenever available, for each account or identifier listed in Attachment A:

a. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers, email addresses (including primary, alternate, rescue, and notification email addresses, and verification information for each email address), the date on which the account was created, the length of service, the IP address used to register the account, account status, associated devices, methods of connecting, and means and source of payment (including any credit or bank account numbers);

b. All records or other information regarding the devices associated with, or used in connection with, the account (including all current and past trusted or authorized iOS devices and computers, and any devices used to access Apple services), including serial numbers, Unique Device Identifiers ("UDID"), Advertising Identifiers ("IDFA"), Global Unique Identifiers ("GUID"), Media Access Control ("MAC") addresses, Integrated Circuit Card ID numbers ("ICCID"), Electronic Serial Numbers ("ESN"), Mobile Electronic Identity Numbers ("MEIN"), Mobile Equipment Identifiers ("MEID"), Mobile Identification Numbers ("MIN"), Subscriber

Identity Modules ("SIM"), Mobile Subscriber Integrated Services Digital Network Numbers ("MSISDN"), International Mobile Subscriber Identities ("IMSI"), and International Mobile Station Equipment Identities ("IMEI");

c. The contents of all emails associated with the account from October 1, 2018 to February 5, 2019, including stored or preserved copies of emails sent to and from the account (including all draft emails and deleted emails), the source and destination addresses associated with each email, the date and time at which each email was sent, the size and length of each email, and the true and accurate header information including the actual IP addresses of the sender and the recipient of the emails, and all attachments;

d. The contents of all instant messages associated with the account from October 1, 2018 to February 5, 2019, including stored or preserved copies of instant messages (including iMessages, SMS messages, and MMS messages) sent to and from the account (including all draft and deleted messages), the source and destination account or phone number associated with each instant message, the date and time at which each instant message was sent, the size and length of each instant message, the actual IP addresses of the sender and the recipient of each instant message, and the media, if any, attached to each instant message;

e. The contents of all files and other records stored on iCloud, including all iOS device backups, all Apple and third-party app data, all files and other records related to iCloud Mail, iCloud Photo Sharing, My Photo Stream, iCloud Photo Library, iCloud Drive, iWork (including Pages, Numbers, Keynote, and Notes), iCloud Tabs and bookmarks, and iCloud Keychain, and all address books, contact and buddy lists, notes, reminders, calendar entries, images, videos, voicemails, device settings, and bookmarks;

f. All activity, connection, and transactional logs for the account (with associated IP addresses including source port numbers), including FaceTime call invitation logs, messaging and query logs (including iMessage, SMS, and MMS messages), mail logs, iCloud logs, iTunes Store and App Store logs (including purchases, downloads, and updates of Apple and third-party apps), My Apple ID and iForgot logs, sign-on logs for all Apple services, Game Center logs, Find My iPhone and Find My Friends logs, logs associated with web-based access of Apple services (including all associated identifiers), and logs associated with iOS device purchase, activation, and upgrades;

g. All records and information regarding locations where the account or devices associated with the account were accessed, including all data stored in connection with Location Services, Find My iPhone, Find My Friends, and Apple Maps;

h. All records pertaining to the types of service used;

i. All records pertaining to communications between Apple and any person regarding the account, including contacts with support services and records of actions taken; and

j. All files, keys, or other information necessary to decrypt any data produced in an encrypted form, when available to Apple (including, but not limited to, the keybag.txt and fileinfolist.txt files).

The Provider is hereby ordered to disclose the above information to the government within 10 days of service of this warrant.

II. Information to be seized by the government

All information described above in Section I that constitutes evidence or instrumentalities of violations of arson of commercial property, in violation of Title 18, United States Code, Section 844(i), conspiracy to commit arson, in violation of Title 18, United States Code, Section 844(m), and destruction, alteration, or falsification of records in federal investigations, in violation of Title 18, United States Code, Section 1519, involving MATTHEW NEUMANN and/or DONALD NEUMANN since October 1, 2018, including, for each account or identifier listed on Attachment A, information pertaining to the following matters:

a. Arson of commercial property, in violation of Title 18, United States Code, Section 844(i), on or about January 2, 2019;

b. Conspiracy to commit arson, in violation of Title 18, United States Code, Section 844(m), occurring on or about January 2, 2019;

c. Destruction, alteration, or falsification of records in federal investigations, in violation of Title 18, United States Code, Section 1519, since on or about January 2, 2019;

d. Preparatory steps taken in furtherance of these crimes;

e. Communications between Matthew Neumann and Donald Neumann;

f. Relationship between Donald Neumann and Matthew Neumann;

g. Use, ownership, custody, control, and cleaning of a 2003 Chevrolet Impala (WI: AEE-6205);

h. Use, ownership, custody, control, damage, or destruction of a 2001 Ford F-250 (WI: MA-9985);

i. Use, possession, custody, or control of the phone number (414) 350-7417;

j. Use, possession, custody, or control of the phone number (414) 687-5095;

k. Use, possession, custody, or control of the phone number (414) 899-6082;

l. Knowledge, use, possession, custody, or control of accelerants, ignitable liquids, or heat sources;

m. Concealment or destruction of evidence of the violations described above;

n. Spot Free Cleaning, a business located in Franklin, Wisconsin, its employees, and its customers;

o. Location, whereabouts, and patterns of travel of Donald Neumann and Matthew Neumann;

p. Appearance or clothing of Donald Neumann or Matthew Neumann on or about January 2, 2019;

q. The identity of the person(s) who created or used the Apple ID, including records that help reveals the whereabouts of such person(s);

r. Evidence indicating how and when the account was accessed or used, to determine the chronological and geographic context of account access, use and events relating to the crime under investigation and the account subscriber;

s. Any records pertaining to the means and source of payment for services (including any credit card or bank account number or digital money transfer account information);

t. Evidence indicating the subscriber's state of mind relating to the crimes under investigation; and

u. Evidence that may identify any co-conspirators or aiders and abettors, including records that help reveal their whereabouts.